

Third Party Application Privacy Impact Assessment

Department of State Privacy Coordinator Sheryl Walter Bureau of Administration Global Information Services Office of Information Programs and Services	
Name of Third Party Application: Sysomos ITAB Number: Determined to not be necessary Month and Year PIA was completed: May 31, 2013	

1) Purpose of the Department of State's use of a third-party website or application. (Henceforth, third-party website or applications will be referred to as third party applications.)

(a) Give a general description of the third party application.

Sysomos is a web-based application that allows searches of publically available content posted to the Internet using products such as Twitter, Facebook, blogs, online news, and other such social media platforms. Sysomos curates this publically available content as a commercial venture, selling access to the database it creates by providing to its users a user interface with which the data can be explored.

Examples of publically available social media information include Tweets, Facebook pages, YouTube videos, Flickr photos, online news and blogs, and other similar online outlets. Such social media information has been broadcast for general public consumption; is available online to members of the general public; is available to the general public free, by subscription, or by purchase; and can lawfully be accessed at any time by any casual observer with Internet access.

Some social media sites give users varying privacy settings to implement preferences with respect to what information is public and what information is subject to controlled dissemination. Information that is marked as subject to controlled dissemination is not considered publically available because it is not available to the general public upon request. Examples of such information include Facebook pages accessible only to certain "friends" or private Tweets. Sysomos collects social media information that is publically available.

The user interface for Sysomos provides a way for end users to search their stored content for items of interest, such as postings about global warming or democracy. Sysomos allows for searches to be in any language or character set. It further provides filters such as time (when something was posted) and location (country). The data Sysomos collects resides on Sysomos systems and is not stored on users' systems.

At this time, the Department of State only has interest in using those aspects of Sysomos pertaining to access to data available to the public over the Twitter platform and data available to the public posted by online news sites.

(b) What is the specific purpose for using the third-party application and how does this purpose assist in accomplishing the Department's mission?

Social media is a key public diplomacy tool in the 21st century. Sysomos can help the Department to maximize its effective use of that tool. It is to be used by the Audience Research and Evaluations Office of the Department's International Information Programs (IIP/ARE) bureau for five (5) main purposes, each of which can be implemented at the global, regional, country, or local level:

1. Understanding how members of foreign publics discuss topics that are of interest to the Department of State so that it can better shape its Public Diplomacy outreach efforts;
2. Understanding the social media response to a planned event, such as a speech by the Secretary of State or the President;
3. Understanding how a planned event was received by the audience(s);
4. Understanding the social media response to an unplanned event, such as a natural disaster, so we can discover how that event is being perceived; and
5. Understanding the reach, resonance, and amplification of our social media outreach efforts so we can better understand how to use social media for communicating to our different audiences.

(c) Is the use of the third-party application consistent with all applicable laws, regulations, and policies?

Yes. The Office of the Legal Adviser has reviewed this proposed use of Sysomos, and the potential legal and policy concerns identified are those addressed by this Privacy Impact Assessment.

(d) What federal authorities permit the collection of information for the intended purpose of this application?

Section 501(a) of the U.S. Information and Educational Exchange Act of 1948 ("Smith-Mundt"), as amended (codified at 22 USC 1461):

The Secretary and the Broadcasting Board of Governors are authorized to use funds appropriated or otherwise made available for public diplomacy information programs to provide for the preparation, dissemination, and use of information intended for foreign audiences abroad about the United States, its people, and its policies, through press, publications, radio, motion pictures, the Internet, and other information media, including social media, and through information centers, instructors, and other direct or indirect means of communication.

Section 604 of the U.S. Information and Educational Exchange Act of 1948 (“Smith-Mundt”), as amended (codified at 22 USC 1469) was most recently amended by Section 1280 the 2012 National Defense Authorization Act (Pub. L. 112-239), which reconstituted the United States Advisory Commission on Public Diplomacy, and assigned the Commission with an annual report that includes an “Effectiveness Assessment”:

In evaluating the public diplomacy and international broadcasting activities described in subparagraph (A), the Commission shall conduct an assessment that considers the public diplomacy target impact, the achieved impact, and the cost of public diplomacy activities and international broadcasting.” (22 USC 1469(d)(1)(B).)

To support this mandate, the statute provides that:

The Secretary of State shall ensure that the Commission has access to all appropriate information to carry out its duties and responsibilities under this subsection. (22 USC 1469(d)(3).

Section 202 of the Foreign Relations Authorization Act, Fiscal Year 1979 (Pub. L. 95–426, codified at 22 USC 1461-1):

The mission of the United States Information Agency [since consolidated with the State Department] shall be to further the national interest by improving United States relations with other countries and peoples through the broadest possible sharing of ideas, information, and educational and cultural activities. In carrying out this mission, the United States Information Agency shall, among other activities—

(1) conduct Government-sponsored information, educational, and cultural activities designed—

(A) to provide other peoples with a better understanding of the policies, values, institutions, and culture of the United States; and

(B) within the statutory limits governing domestic activities of the Agency, to enhance understanding on the part of the Government and people of the United States of the history, culture, attitudes, perceptions, and aspirations of others;

2) Personally Identifiable Information (PII) available through the use of the third-party application.

(a) What PII will be made available to the Department?

The response queries provided by Sysomos may contain Twitter handles. Individual data elements may include Twitter handles, location (such as city or IP address), and Tweet contents, any of which has the potential to be PII depending on the content of each field for each user.

The information returned by Sysomos in response to a user query generally includes the user name, time, location, and the actual contents of the message.

(b) What are the sources of the PII?

Individual users of Twitter create a Twitter username, and have the option of providing further profile information that could include personal data. Users are then free to post Tweets. By using Twitter, users agree to a Terms of Service and a Privacy Policy that grant Twitter a license to further distribute the contents of public Tweets and non-privacy-restricted profile data. Twitter sells access to this information to services such as Sysomos by providing electronic access to the live Twitter feed and raw profile data.

(c) From which individuals is the information collected?

The Twitter data comes from members of the public, including individuals and organizations, who have joined the Twitter service and who have not made their Tweets private.

(d) Does this collection of information require compliance with the Paperwork Reduction Act (PRA) and, if so, how will the Department comply with the statute?

This does not constitute a collection under the Paperwork Reduction Act.

3) Intended or expected use of PII

(a) How will the Department use the PII described in Section 2 above?

The Department of State does not intend to use the limited PII gathered in Sysomos in any way.

(b) Provide specific examples of how the PII may be used.

The Department of State does not intend to use the limited PII gathered in Sysomos in any way.

4) Sharing or disclosing PII

(a) With what entities or persons inside or outside the Department will the PII be shared and for what purpose will the PII be disclosed?

The only persons with access to PII to Sysomos will be those within IIP/ARE who authorized to do so as part of their official duties.

(b) How will the PII be transmitted or disclosed to internal or external entities or persons?

Most analyses and reports will not contain PII. When information that is more detailed is required, including PII, it is shared in a format that cannot be edited or disaggregated, such as PDF, and further only shared with internal entities whose access to such content is part of their official duties. Providing documents in a locked format, such as PDF,

prevents recipients from manipulating the contents or storing the contents in some other way.

(c) What safeguards will be in place to prevent uses other than those legally authorized and described in this PIA?

Access to the Sysomos tool is password protected, and the password is given only to those whose official duties include the functions enabled by Sysomos. All personnel are required to complete privacy training. Further, in using the Sysomos tool, and for purposes of this document and the commitments it contains, the Department will treat Twitter user names (known as handles) as PII, and will do so unless and until further guidance on this issue is conveyed by the Department. We will abide by the following standard privacy rules found at

[http://a.m.state.sbu/sites/gis/ips/prv/About Us/Rules of Behavior for Protecting PII.aspx](http://a.m.state.sbu/sites/gis/ips/prv/About%20Us/Rules%20of%20Behavior%20for%20Protecting%20PII.aspx):

- Do not inspect, search, or browse records of PII in files or databases unless you are authorized to do so in the performance of your official duties and you have a need to do so to accomplish your assigned work.
- Do not alter or delete records containing PII unless it is necessary in the performance of your official duties.
- Do not copy records of PII to a non-government furnished computer.
- Do not disclose PII to others, including other authorized users, verbally or otherwise unless there is a need to do so in the performance of your official duties.
- Do not reveal your password to others or allow them to log on under your account.
- Do not leave your work area without first locking your computer.
- Do not store PII in shared electronic folders or shared network files.
- Do not email PII in an unencrypted form without first evaluating the potential harm to the individuals if their PII were exposed.
- Do not leave hard copy PII records exposed and subject to theft.

In addition, we will not run a report on the Sysomos tool that allows it to pull up a list of “influencers,” such as the list of handles that received the most mentions in tweets on a particular topic, and that any reports pulled from Sysomos will be based on topic searches, not searches based on user names.

We also agree that no one with access to Sysomos will attempt in any other way to collect or analyze data on “influencers” or otherwise attempt to “drill down” (perform analysis) on the handles or other identifying information of Tweeters that may appear in the Sysomos reports it pulls, unless and until there is Department agreement on how that may be done.

Finally, all staff who will be using this tool have received the mandatory online “Protecting Personally Identifiable Information (PII)” (PA459) training.

5) Maintenance and retention of PII

(a) How will the Department maintain the PII and for what time period?

Printed reports from Sysomos, stored as both hard copy and electronic PDFs, will be retained only as long as relevant, with such relevance reviewed at least every six months, such that the total retention period shall in no case extend beyond two years.

(b) Is there a records disposition schedule covering this collection? If so, what is the retention period?

Per Records Management, no official records schedule is required.

6) Securing PII

(a) Will the Department's privacy and security officials collaborate to develop methods for securing PII?

Yes. Methods include keeping reports in locations only accessible by those authorized to have such access as part of their official duties.

(b) Describe how a user will access the third party application.

Department of State users access the system through a web-based user interface that allows users to create and conduct searches for content of interest. Access to this system is password protected, and passwords are only available to those authorized to have such access as part of their official duties. There is no other access to the database.

The Department of State only accesses the Sysomos system for analysis of publically broadcast Twitter postings and online news outlets. Data and information collected from other platforms by the Sysomos system are not being analyzed by the Department of State.

7) Identifying and mitigating other privacy risks

What other privacy risks exist and how will the Department mitigate those risks?

1. Users tracking back Twitter handles and following or contacting individuals is mitigated by established policy against such a practice and by clearly communicating that policy to all who have access to Sysomos reports.
2. Users using information for a purpose it was not intended is mitigated by requiring persons authorized to operate the Sysomos system to complete the online course "Protecting Personally Identifiable Information (PII)" as previously mentioned.
3. Users violating any aspect of the PII guidelines shall be subject to standard Department of State protocols, including warnings, official letters of reprimand, and removal of access privileges.

8) Creating or modifying a system of records

(a) Is there an existing system of records to cover this collection of records as required under the Privacy Act of 1974?

No system of records is created by this use of Sysomos, so a SORN is not required.

(b) If “yes” to the question above, which system of records notice (SORN) covers this collection? (For a list of all Department published SORNS, go to www.state.gov/m/a/ips/c25533.htm).

If there is no existing Department SORN to cover this collection, one must be created. Please contact SornTeam@state.gov for guidance.

(c) Is notice provided to the record subjects, other than through the SORN (e.g., through a Privacy Act statement or privacy notice)?

Notice is provided through this PIA, which will be published on the public Department of State website.